**Wdrożenie systemu do zarządzania produkcją w kontekście normy ISO27001 oraz dyrektywy NIS2**

**W minionym roku mogliśmy usłyszeć o wielu incydentach związanych z wyciekiem lub utratą danych, jakie miały miejsce w polskich przedsiębiorstwach. Niestety takich zdarzeń jest coraz więcej i to pomimo rosnącej świadomości użytkowników oraz ciągłego wzrostu nakładów na cyberbezpieczeństwo.**

Aby zminimalizować prawdopodobieństwo wystąpienia incydentu oraz ograniczyć jego wpływ na funkcjonowanie organizacji, część firm, nie czekając na wejście w życie regulacji prawnych zobowiązujących je do uruchomienia systemu zarządzania bezpieczeństwem informacji (SZBI), zdecydowała się wcześniej wdrożyć takie rozwiązanie bazując na wytycznych, jakie daje norma ISO 27001 [1]. Ponieważ mówimy tutaj o środkach organizacyjnych i technicznych mających objąć całość przedsiębiorstwa, nie mogą zostać pominięte systemy wspomagające zarządzenie produkcją takie jak [MES](https://www.eqsystem.pl/system-mes-na-co-zwrocic-uwage-przy-wyborze/) (Manufacturing Execution System), [APS](https://www.eqsystem.pl/product/asprova/) (Advanced Planning and Scheduling) czy [CMMS](https://www.eqsystem.pl/product/xprimer-cmms-wsparcie-utrzymania-ruchu/) (Computerised Maintenance Management System). Dzieje się tak dlatego, że korzystają one z danych, które są kluczowe z punktu widzenia ciągłości działania procesów produkcyjnych, nawet jeżeli same systemy fizycznie znajdują się poza infrastrukturą IT organizacji.

Jednym z podstawowych założeń każdego systemu SZBI jest regularne zarządzanie ryzykiem związanym z zasobami, które obejmuje. Poprzez zarządzanie ryzykiem rozumie się identyfikację możliwych zdarzeń zagrażających bezpieczeństwu informacji, ocenę prawdopodobieństwa i skutków takiego zdarzenia oraz podjęcie odpowiednich działań mających je zminimalizować. W przypadku gdy mowa jest o projekcie wdrożenia nowego rozwiązania IT, to już na etapie wyboru oprogramowania i dostawcy należy przeprowadzić taką ocenę obejmującą sam produkt, jego producenta oraz firmę, która miałaby dane rozwiązanie wdrażać w organizacji.

**Bezpieczeństwo informacji i incydenty**

Bezpieczeństwo informacji rozumiemy jako zapewnienie nienaruszalności trzech składowych: poufności, dostępności i integralności danych. Jest to tzw. triada CIA – Confidentiality, Integrity, Availability. Poufność oznacza, że dostęp do informacji mają tylko osoby, które są do tego upoważnione. Jako dostępność rozumiemy możliwość korzystania z informacji wtedy, gdy jest ona niezbędna. Integralność z kolei oznacza kompletność i prawdziwość danych. Z incydentem bezpieczeństwa informacji będziemy mieli do czynienia przy każdym zdarzeniu związanym z faktem lub uzasadnionym podejrzeniem naruszenia jednej z trzech powyżej opisanych składowych. Mając tak zdefiniowane pojęcia łatwiej jest wyobrazić sobie, na co trzeba zwrócić uwagę przy określaniu potencjalnych zagrożeń i możliwych środków zapobiegawczych.

Warto zaznaczyć w tym miejscu, że bezpieczeństwo informacji opiera się na filarach, którymi są: ludzie, procedury i rozwiązania technologiczne. Niestety to człowiek jest zazwyczaj tym najsłabszym ogniwem i dlatego wymaga uwagi oraz odpowiedniego przygotowania. Wdrożenie dużego systemu informatycznego to stres związany z odpowiedzialnością nie tylko za uruchomienie nowego rozwiązania, ale też za utrzymanie ciągłości działania zainteresowanej komórki w etapie przejściowym. W połączeniu z naciskiem na dotrzymanie terminów może to przyczynić się do utraty koncentracji, a tym samym do błędu lub zwykłego niedopatrzenia.

**Zakres danych, jakimi posługują się systemy MES, CMMS i APS**

Szczegółowe informacje mówiące o tym jakimi danymi posługuje się wdrażany system IT i z jakimi innymi systemami są one wymieniane, zazwyczaj dostarczane są przez dostawcę rozwiązania po zakończeniu analizy przedwdrożeniowej. Możemy jednak założyć, że dane, którymi posługuje się każdy system klasy MES i APS dzielimy na dwie grupy: dane osobowe i dane mające znaczenie biznesowe.

Często pracownicy realizując swoje zadania w systemie MES posługują się swoim nazwiskiem, natomiast w przypadku monitorowania pracy działu utrzymania ruchu przy użyciu CMMS, jest to po prostu konieczność. Dane te objęte są prawnym obowiązkiem ochrony na mocy Rozporządzania Parlamentu Europejskiego nr 2016/267 znanego jako RODO [2]. Ponadto informacje te mogą czasem mieć wartość dającą przewagę konkurencyjną np. w przypadku wymaganej obszernej wiedzy specjalistycznej na konkretnym stanowisku pracy.

Warunkiem utrzymania wspomnianej przewagi konkurencyjnej jest zachowanie w tajemnicy wiedzy o możliwościach produkcyjnych zakładu. Informacje o nich przetwarzane są m.in. przez systemy klasy ERP, MES i APS w postaci zapisów obejmujących m.in. technologie produkcji, wielkości oraz składniki parku maszynowego oraz wolumeny, na które opiewają zlecenia produkcyjne. Zdarza się, że w systemie MES w powiązaniu ze zleceniem produkcyjnym występują również niezakodowane nazwy klientów. W połączeniu z wcześniej wymienionymi danymi są to informacje, które ujawnione publicznie lub przechwycone przez konkurencję mogą ostatecznie doprowadzić do wyeliminowania firmy z rynku.

**Odpowiedzialność prawna zamawiającego**

Częścią każdego projektu, do którego zatrudniani są zewnętrzni dostawcy, są odpowiednie zapisy umowne mające zobowiązać podmiot zewnętrzny do należytego wykonania zlecenia przy uwzględnieniu bezpieczeństwa informacji niejawnych. Warunki te obwarowane są wysokimi karami umownymi mającymi to zagwarantować. Niestety zabezpieczenia prawne, takie jak umowa NDA (Non Disclosure Agreement) oraz zapisy dotyczące bezpieczeństwa informacji w pozostałych umowach, choć są niezbędne, nie dają 100% pewności, że dane będą bezpieczne i nie zdejmują odpowiedzialności za skutki incydentów z podmiotu zlecającego. Niektóre z przepisów prawa dotyczących zarządzania bezpieczeństwem informacji mówią o tym wprost.

W przypadku danych osobowych to administrator jest odpowiedzialny za bezpieczeństwo danych i zobowiązany jest do ich przetwarzania z uwzględnieniem odpowiednich środków zabezpieczających, o czym mówi art. 24.§1 RODO. Dotyczy to także sytuacji, gdy przetwarzanie jest zlecane firmie zewnętrznej na podstawie odpowiedniej umowy powierzenia. Prezes Urzędu Ochrony Danych Osobowych podkreśla to w uzasadnieniach dla kar administracyjnych nakładanych na mocy art. 83 RODO na podmioty zlecające przetwarzanie. Warto przypomnieć, że w myśl paragrafu 1. przytoczonego artykułu kary powinny być „skuteczne, proporcjonalne i odstraszające”.

Wspomniany na wstępie artykułu obowiązek wdrożenia SZBI wynika z przygotowywanej nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa [3]. Nowelizacja ta ma zaimplementować do polskiego porządku prawnego obowiązującą już dyrektywę PE 2022/2555 „W sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa”, tzw. NIS2 [4]. W porównaniu do poprzednich wersji dyrektywy NIS i ustawy o KSC znacząco poszerza się katalog branż, których regulacje będą dotyczyć, definiując jednocześnie grupy podmiotów kluczowych i ważnych. Z lektury załączników do projektu wspomnianej ustawy wynika, że do grup tych kwalifikuje się większość firm produkcyjnych używających lub zainteresowanych wdrożeniem oprogramowania klasy MES i APS. W myśl art. 8c projektu nowelizacji to najwyższe kierownictwo podmiotu wg definicji z ustawy w o rachunkowości [5], czyli członkowie Zarządu, odpowiadają osobiście za dochowanie obowiązków związanych z bezpieczeństwem informacji w podmiotach z grupy kluczowych lub ważnych. Dzieje się tak również wtedy, gdy obowiązki w tym zakresie zostały delegowane na inne osoby. Dyrektywa NIS2 oraz wprowadzająca ją ustawa przewidują, podobnie jak w przypadku RODO, wysokie kary finansowe dla podmiotów niespełniających wymagań dotyczących zarządzania bezpieczeństwem informacji.

Dodatkowym źródłem odpowiedzialności strony zamawiającej wdrożenie rozwiązania IT są oczywiście wszelkie zobowiązania wynikające z umów z interesariuszami. Patrząc z tej perspektywy role się odwracają i teraz to organizacja będąca zamawiającym wdrożenie systemu musi zadbać o to, aby być wiarygodnym partnerem biznesowym dla swoich klientów, nie tylko pod kątem rzetelnej realizacji zamówień, ale też bezpieczeństwa powierzonych i przetwarzanych informacji.

**Wdrożenie systemów IT w kontekście systemu zarządzania bezpieczeństwem informacji**

Bez względu na to, czy w organizacji zamierzającej wdrożyć nowy system MES lub APS funkcjonuje system zarządzania bezpieczeństwem informacji zbudowany w oparciu o normę ISO 27001, czy jeszcze nie, warto przy implementacji nowego rozwiązania posłużyć się wskazówkami, które w tym kontekście dostarcza przywołana norma. Punkt 5.8 załącznika A do normy ISO27001 wymaga, aby bezpieczeństwo informacji było uwzględniane przy zarządzaniu projektami, a sama norma mówi, że podejmowane działania powinny być oparte o zarządzanie ryzykiem. Ważne jest, aby zagadnienia te były brane pod uwagę od samego początku, czyli etapu przygotowania projektu, jeszcze przed formalnym startem przedsięwzięcia. Podejście takie zalecają również powszechnie stosowane metodyki prowadzenia projektów, takie jak PRINCE2 czy PMBOK.

Pierwszym i jednym z najważniejszych kroków w opartym o ryzyko zarządzaniu projektem IT jest inwentaryzacja zasobów informacyjnych, których wdrożenie dotyczy oraz możliwych ryzyk z nimi związanych. Należy przy tym uwzględnić elementy systemów informatycznych, w których informacje są pozyskiwane i przetwarzane, poszczególne fazy wdrożenia oraz produkcyjnego użytkowania systemu, a także persony mające mieć do nich dostęp. Dla tak skomponowanej listy identyfikujemy możliwe zdarzenia mogące zakłócić jeden ze składników triady CIA, a następnie szacujemy poziom ryzyka będący wypadkową prawdopodobieństwa wystąpienia zdarzenia oraz konsekwencji możliwych negatywnych skutków. Innymi słowy tworzymy rejestr ryzyk. Do realizacji tego zadania należy wyznaczyć wewnętrzny zespół składający się m.in. z kierownika projektu, osoby odpowiedzialnej za utrzymanie systemu bezpieczeństwa informacji, przedstawiciela działu zajmującego się utrzymaniem firmowych systemów informatycznych oraz osób zajmujących się bezpośrednio produkcją, takich jak: planista, technolog oraz kierownik produkcji.

Na tym etapie widać już obszary, na które należy zwrócić szczególną uwagę podczas dalszych prac nad projektem i jakie należy podjąć działania, aby maksymalnie zredukować prawdopodobieństwo wystąpienia oraz skutki potencjalnego incydentu. Warto w tym miejscu posłużyć się listą punktów kontrolnych z załącznika A normy ISO27001 tak, aby pokryć zabezpieczenia z wszystkich czterech grup – technologicznych, fizycznych, osobowych i organizacyjnych. Te ostatnie związane są z przydzielaniem ról w zespołach projektowych dostawcy i zamawiającego oraz zakresem informacji, do których te osoby powinny mieć dostęp. Szczególny nacisk należy położyć na minimalizację tych zakresów do niezbędnego minimum wg zasady POLP (Principle of Least Privilege).

Z lektury tak sporządzonego rejestru ryzyk wynikać będzie również, czy obecne założenia projektu, w tym funkcjonalności wdrażanego systemu, spełniają wymagania stawianych regulacji prawnych takich jak RODO i NIS2. Na bazie powyższych powinno się sporządzić listę kontrolną i skonfrontować ją z możliwościami potencjalnych rozwiązań oraz ich dostawców. Sam rejestr ryzyk projektu powinien być dokumentem aktualizowanym na bieżąco w trakcie trwania całego procesu wdrożenia, aby stać się ostatecznie częścią rejestru ryzyk SZBI w momencie produkcyjnego uruchomienia oprogramowania.

**Wymagania stawiane producentom oprogramowania i firmom wdrożeniowym**

Przed rozpoczęciem projektu wdrożeniowego z zewnętrznym dostawcą należy już na etapie wyboru potencjalnego partnera sprawdzić, czy posiada on odpowiednie kompetencje w zakresie zarządzania bezpieczeństwem informacji. W każdej organizacji, która uruchomiła oraz certyfikowała SZBI wg normy ISO 27001 zasady zarządzania bezpieczeństwem informacji funkcjonują na co dzień i są częścią jej kultury. Organizacja taka wdrożyła już odpowiednie środki organizacyjne i techniczne oraz dba o wysoki poziom świadomości cyberbezpieczeństwa u swoich pracowników m.in. poprzez regularne szkolenia. Co więcej, zgodnie z wymaganym normą schematem PDCA, wszystkie powyższe działania są na bieżąco monitorowane i udoskonalane.

Najprostszą i najszybszą metodą oceny wiarygodności potencjalnego dostawcy na tym etapie projektu jest więc sprawdzenie, czy dany podmiot posiada aktualny certyfikat wdrożenia ISO 27001 wydany przez renomowaną jednostkę certyfikującą i czy certyfikacja obejmuje zakres zarządzania projektami wdrożeniowymi. W przypadku wdrożenia systemu MES lub APS jest to niezwykle istotne, gdyż, jak wykazano powyżej, konsultanci firmy wdrożeniowej będą pracować na danych krytycznych z punktu widzenia przedsiębiorstwa będącego klientem. Każdy taki dostęp powinien zatem odbywać się w sposób opisany i kontrolowany odpowiednim regulaminem, procedurami oraz instrukcjami.

Ostateczny wybór warto poprzedzić przeprowadzeniem audytu u potencjalnego partnera biznesowego w zakresie zagadnień związanych z cyberbezpieczeństwem, również w obszarze zarządzania projektem oraz sprawdzić podczas wizyty referencyjnej, jak powyższe zagadnienia zostały zaopiekowanie u jego obecnych klientów.

**Podsumowanie**

Wdrożenie systemu wspomagającego zarządzenie produkcją, takiego jak MES czy APS, jest dużym przedsięwzięciem wymagającym współpracy wielu interesariuszy wewnętrznych oraz zewnętrznych. Poziom złożoności takiego projektu z natury generuje więc wiele ryzyk związanych z bezpieczeństwem informacji. Pochodzą one zarówno z przebiegu samego procesu wdrożeniowego, wykorzystanych technologii, jak i funkcjonalności wdrażanego systemu. Bez względu jednak na źródła, wspomniane ryzyka powinny zostać zidentyfikowane na etapie przygotowania projektu i odpowiednio zarządzane podczas trwania wdrożenia, zarówno przez zamawiającego, jak i dostawcę. Tylko takie podejście pozwala zminimalizować prawdopodobieństwo wystąpienia incydentów bezpieczeństwa oraz ograniczyć do akceptowalnego minimum ich ewentualne skutki. Jest to niezwykle istotne, gdyż prawidłowo wdrożony system MES lub APS powinien przynieść poprawę wydajności procesów produkcyjnych, ale też poprawne funkcjonowanie tych systemów może okazać się warunkiem ciągłości działania całego przedsiębiorstwa.

Jest to jeden z powodów, dla którego tak ważny jest nie tylko wybór odpowiedniego systemu, ale też zaufanego dostawcy, czyli takiego, który potrafi wykazać, że poważnie traktuje zagadnienia związane z cyberbezpieczeństwem. Dowodem na takie podejście jest z całą pewnością działający w organizacji certyfikowany system zarządzania bezpieczeństwem informacji oparty o normę ISO 27001. Należy również pamiętać, że nie można oddelegować całej odpowiedzialności w tym zakresie na dostawcę. Pomijając obowiązki nakładane przez przepisy prawa, to ścisłe kierownictwo organizacji będącej klientem odpowiada za jej efektywne funkcjonowanie i dlatego też musi zadbać, aby strona zamawiająca aktywnie nadzorowała proces wdrożenia, także pod kątem bezpieczeństwa informacji.

Warto w tym miejscu podkreślić raz jeszcze korzyści wynikające z wdrożenia i certyfikacji normy ISO 27001 w organizacji. Porządkuje ono zagadnienia związane z bezpieczeństwem informacji we wszystkich obszarach działalności przedsiębiorstwa. Tworzy przejrzyste procedury i instrukcje postepowania również w przypadku wyboru nowych systemów, realizacji projektów wdrożeniowych i późniejszej eksploatacji. Podejście oparte o zarządzenie ryzykiem nie tylko znacznie ułatwia wybór docelowych rozwiązań, ale sprawia też, że w dłuższej perspektywie będą to wybory uzasadnione ekonomiczne.

Łukasz Widera, ekspert ds hardware i IoT w dziale analiz eq system

**Przypisy**

l PN-EN ISO/IEC 27001:2023-08 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności, Systemy zarządzania bezpieczeństwem informacji, Wymagania”

l ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

l https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/902927\_projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw.html

l [DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)

l Ustawa z dnia 29 września 1994 r. o rachunkowości Dz.U. 1994 nr 121 poz. 591, art. 3 ust. 1 pkt 6